(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2003233521 A
(43) Date of publication of application: 22.08.2003

(51) Int. Cl G06F 12/00
G06F 11/00, G06F 12/14

(21) Application number: 2002034804
(22) Date of filing: 13.02.2002

(71) Applicant: HITACHI LTD
(72) Inventor: ARAI MASATO
UMETSU TOSHIKAZU

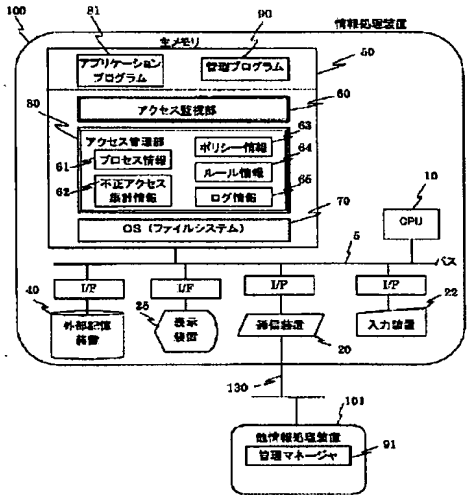
(54) FILE PROTECTION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a file protection system capable of detecting illicit access regarded to be malicious by the monitoring result of file access in real time for prohibiting the illicit access and preventing illicit operation caused afterward.

SOLUTION: Among file accesses monitored by an access monitoring part 60, an access management part 80 rejects a file access violating access policy information 63, and at the same time, the access is recorded as abnormal access summarization information 62. If the summarization information satisfies a criterion defined by rule information 64, it is regarded that there exists an illicit access having malicious intention, and protection processing defined by the rule information 64 is carried out by the access management part 80 for preventing the following illicit operation.

図1



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－233521
（P2003－233521A）
(43)公開日　平成15年８月22日(2003.8.22)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	12/00	５３７	Ｇ０６Ｆ 12/00	５３７Ｚ	５Ｂ０１７
	11/00		12/14	３１０Ｋ	５Ｂ０７６
	12/14	３１０		３２０Ａ	５Ｂ０８２
		３２０	9/06	６６０Ｎ	

審査請求　未請求　請求項の数13　ＯＬ　（全 17 頁）

(21)出願番号　特願2002－34804(P2002－34804)

(22)出願日　平成14年２月13日(2002.2.13)

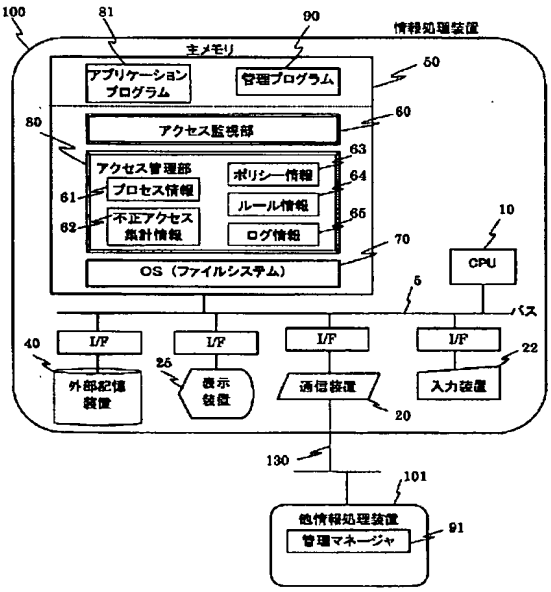
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　荒井　正人
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　梅都　利和
愛知県尾張旭市晴丘町池上１番地　株式会社日立製作所情報機器事業部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ファイル保護システム

(57)【要約】
【課題】ファイルアクセスの監視結果から悪意があると思われる不正アクセスをリアルタイムに検出し、当該アクセスを禁止すると共に、以後発生する不正行為まで阻止可能なファイル保護システムを提供する。
【解決手段】アクセス監視部６０が監視するファイルアクセスのうち、ポリシー情報６３に違反したものをアクセス管理部８０により阻止すると同時に、異常アクセス集計情報６２にて記録する。上記集計情報がルール情報６４にて規定した判定基準を満たした場合には、悪意をもつ不正アクセス主体が存在すると見なして、同じくルール情報６４にて定義された防御処理をアクセス管理部８０により実行し、以後の不正行為を防止する。

図１



1

【特許請求の範囲】

【請求項１】ファイルシステムを備えた情報処理装置において、

ファイルアクセスの監視および制御処理を行うアクセス制御手段と、

正常アクセスと異常アクセスを区別するためのポリシー情報と、

異常アクセスのなかから不正アクセスを区別するための判定基準を備え、

前記アクセス制御手段は、

前記ポリシー情報を用いて異常アクセスを検出する手段と、

前記判定基準を用いて不正アクセスを検出する手段と、

前記異常アクセスと不正アクセスの実行を防止する手段を備えるファイル保護システム。

【請求項２】請求項１のファイル保護システムにおいて、

前記異常アクセス検出手段と、前記不正アクセス検出手段とが検出した異常アクセスおよび／または不正アクセスについて証跡を記録する手段を備えるファイル保護システム。

【請求項３】請求項１のファイル保護システムにおいて、

前記アクセス制御手段は、第１段階として、前記異常アクセス検出手段を用いて異常アクセスを検出し、第２段階として、前記不正アクセス検出手段を用いて異常アクセスの中から不正アクセスを検出するファイル保護システム。

【請求項４】請求項３のファイル保護システムにおいて、

前記ポリシー情報は、正常なアクセスを定義し、および／または、

前記判定基準は、不正アクセスを検出するため、不正アクセスを定義した不正アクセス判定基準であるファイル保護システム。

【請求項５】請求項４のファイル保護システムにおいて、

さらに、前記不正アクセス判定基準を満たした場合に実行すべき防御処理を定めたルール情報を備え、

前記アクセス制御手段は、

前記不正アクセス検出手段が不正アクセスを検出した場合に、前記ルール情報に従い前記防御処理を実行する防御処理手段を備えるファイル保護システム。

【請求項６】請求項５のファイル保護システムにおいて、

前記ポリシー情報は、記憶装置名、ボリューム名、ドライブ名、ディレクトリ名、ファイル名のいずれか、あるいはそれらの組み合わせで表記された保護対象の名称と、当該保護対象に対する正常なアクセスの条件を記述したものであるファイル保護システム。

2

【請求項７】請求項６記載のファイル保護システムであって、

前記ポリシー情報はさらに、当該保護対象の重要度を記述したものであり、

前記不正アクセス判定基準において、保護対象の重要度Ｌと、異常アクセス回数Ｎと、有効期間Ｔとを指定し、前記重要度Ｌを割り当てられた１つ以上の保護対象に対して、前記有効期間Ｔ内に、前記異常アクセスが前記Ｎ回以上発生した場合を不正アクセスと定義するファイル保護システム。

【請求項８】請求項６記載のファイル保護システムであって、

前記不正アクセス判定基準において、保護対象の名称Ｆと、異常アクセス回数Ｎと、有効期間Ｔとを指定し、前記名称Ｆの保護対象に対して、前記有効期間Ｔ内に、前記異常アクセスが前記Ｎ回以上発生した場合を、不正アクセスと定義するファイル保護システム。

【請求項９】請求項５記載のファイル保護システムであって、

前記ポリシー情報を複数備え、

前記防御処理手段は、

前記ポリシー情報の切り替え処理手段と、管理者への通知処理手段と、複数の防御処理の中から１つ以上の処理を実行する手段を備えるファイル保護システム。

【請求項１０】請求項６記載のファイル保護システムであって、

前記アクセス制御手段は、さらに、実行中のプログラムの監視処理手段を備え、

前記不正アクセス判定基準において、異常アクセス回数Ｎと、有効期間Ｔとを指定し、前記有効期間Ｔ内に、同一の実行中プログラムから、前記異常アクセスが前記Ｎ回以上発生した場合を、不正アクセスと定義するファイル保護システム。

【請求項１１】請求項９記載のファイル保護システムであって、

前記防御処理手段は、さらに、前記実行中プログラムの処分手段を備え、

前記実行中プログラムの処分手段は、

前記実行中プログラムによる以後のアクセスを禁止するアクセス禁止処理手段と、

前記実行中プログラムを終了させる強制終了処理手段と、

前記実行中プログラムによる以後のアクセスを全てダミーファイルへのアクセスに変換して当該アクセスを監視および／または記録する監視記録処理手段と、

前記アクセス禁止処理手段、前記強制終了処理手段、または前記監視記録処理手段のいずれかを実行する手段を備えるファイル保護システム。

【請求項１２】請求項３記載のファイル保護システムであって、

当該ファイル保護システムの管理者に、不正なアクセスの発生状況を提供する手段と、
前記管理者から実行中プログラムの強制終了処理、ポリシー切り替え処理、ルール設定処理から任意の処理の実行指示を受け付ける手段を備えるファイル保護システム。
【請求項１３】請求項１記載のファイル保護システムにおいて、
前記アクセス制御手段は、さらに、プログラムの起動の監視手段を備え、
前記ポリシー情報は、前記情報処理装置にて利用可能なプログラムの名称と、当該プログラムからの正常なアクセスの条件を定義し、
前記アクセス制御手段は、
プログラムの起動を検知して前記ポリシー情報と照合し、前記ポリシー情報に登録されていないプログラムの起動であった場合に当該プログラムの起動を防止する処理手段と、
当該プログラムが、前記ポリシー情報に登録されているプログラムであった場合には、当該プログラムからのファイルアクセスを前記ポリシー情報と照合し、適合したファイルアクセスの実行を許可する手段を備えるファイル保護システム
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータシステムが管理する情報資産を不正なアクセスから保護する場合に好適なファイル保護方法に関する。
【０００２】
【従来の技術】情報ネットワークシステムにて発生し得るセキュリティ脅威は、ネットワークを経由して外部から攻撃するケースと、情報資産が格納されたホストを内部にて直接操作して攻撃するケースとに大別できる。このような攻撃から情報資産を保護する策として、ファイアウォールによるネットワークレベルのアクセス制御機能や、ホストに搭載したＯＳ(Operating System)が備えるファイルアクセス制御機能を用いるのが一般的である。また、攻撃に用いられるパケットの既知の特徴（プロトコルヘッダー中のポート番号や、データ部分の内容など）を用いたパターン照合により、ネットワーク上のパケットを分析し、不正アクセスと思われるパケットを検出してアラームを発したり、ファイアウォールやルータの設定を変更したりすることにより、不正と思われる通信を積極的に検出し、その場で遮断するといった不正アクセス監視技術もある。更に、どのようなパケットが通過したのかをログ情報として記録、保存しておくことで、後日問題が発覚した場合に追跡調査も可能となる。
【０００３】不正行為の目的には様々なものがあると予想できるが、情報ネットワークシステムにおいて最も重要な保護対象は、ファイルやデータベースに格納された情報資産であることから、不正行為を阻止するためには、情報資産に対する直接的なアクセスも監視し、不正なアクセスの検知と防御ができることが望まれる。このような技術には、前述のようにＯＳが備えるファイルアクセス制御機能が代表的なものとして挙げられる。
【０００４】これは、予め各ファイルに対する正常なアクセスを、情報資産（ファイル名）と、アクセスタイプ（read, write, execute）と、アクセス元（ユーザー名、グループ名）を組み合わせたパーミッション情報として定義しておき、正常でない、つまり異常なアクセスを遮断するものである。また、ファイルへのアクセスを監視し、異常なアクセスを検出すると当該ファイルのパーミッション情報を変更する方法が、米国特許5919258号に開示されている。
【０００５】
【発明が解決しようとする課題】先に述べた異常アクセスは、不用意（過失）によるものと故意（悪意）によるものとに大別できる。上記特開平9-218837号公報にて開示しているファイルアクセスの監視方法では、異常なファイルアクセスを１度でも検出するとアクセスパーミッションを変更するため、正規のユーザーによる誤ったファイル操作であっても、例えば共有ファイルが他のユーザーから一時的に利用できなくなる可能性がある。つまり、ファイル保護の観点からは有効であるが、不用意なファイルアクセスによって通常業務に支障をきたす点で問題がある。
【０００６】一方、異常なファイルアクセスを発行したアクセス主体（実行中のプログラムまたはプロセス）が、真に悪意をもつものであれば、ファイルアクセス以外にもどのような不正行為を働くか予想できない。このような異常なファイルアクセスを試みた実行中プログラム（プロセス）を放置しておくと、やがてＯＳやプログラムに潜在するセキュリティホールを発見し、監視の目を潜り抜け、悪意を持ってアクセスしてくる恐れもある。
【０００７】従って、改善されたファイル保護システムが望まれている。
【０００８】
【課題を解決するための手段】本発明は、ファイルアクセスを監視し、その結果から悪意の有無を判断するファイル保護システムを提供する。
【０００９】さらに、悪意があると判断するアクセスを検出した場合、当該アクセスを禁止すると共に、以後発生する不正行為を阻止するための防御処理を実行するファイル保護システムを提供する。これにより、情報資産をより安全に利用することが可能になる。
【００１０】通信を例にとって説明した、従来の不正アクセス監視技術は、通信データや通信量、アプリケーションで使用されるコマンドといった情報から不正と思われる行為の有無を検知するものであり、その行為が真に

不正なものかどうかまでを監視するものではない。これに対し、本発明によるファイル保護システムは、さらに、上記異常なファイルアクセスを発行したアクセス主体が働くかもしれない不正行為に対して先手を打つために、上記アクセス主体そのものの行為を制限するファイル保護システムを提供する。

【００１１】なお、本明細書においては、正常なアクセスではないアクセスを「異常アクセス（unauthorized access）」といい、異常アクセスの内、悪意によるアクセスを「不正アクセス（malicious access）」という。

【００１２】本発明のファイル保護システムは、正常アクセスと異常アクセスを区別するためのアクセス制御ポリシー情報（ポリシー情報という）と、不正アクセスとそうではない異常アクセスを区別するための判定基準を備える。より具体的に、アクセス制御ポリシー情報は正常なアクセスを定義するものであって良い。判定基準は、不正アクセスを検出するための不正アクセス判定基準であって良い。

【００１３】本発明のファイル保護システムは、第１段階として、ポリシー情報を用いて異常アクセスを検出し、第２段階として不正アクセス判定基準を用いて異常アクセスの中から不正アクセスを検出する。

【００１４】本発明のファイル保護システムによれば、ファイルシステムを備えた情報処理装置は、ファイルアクセスの監視と制御処理を行うアクセス制御部と、正常なアクセスを規定したアクセス制御ポリシー情報と、悪意のある行為かどうかを判断するための不正アクセス判定基準、および当該基準を満たした場合に実行すべき処理について記述したルール情報とを備える。上記アクセス制御部は、上記情報処理装置におけるファイルアクセスの監視結果が、上記ルール情報に記述された不正アクセス判定基準に達した場合に、同じく上記ルール情報に記述された所定の処理を実行することにより、上記ファイルアクセスの要求元となるプログラムからの以後のアクセスを制限することを特徴とする。

【００１５】上記アクセス制御ポリシー情報は、保護対象となるファイルの名称およびその重要度と、当該ファイルに対する正常アクセスの条件を記述したものであり、当該正常アクセスの条件を満たさないアクセスを上記アクセス制御手段が検出した場合は、当該アクセスを異常アクセスとみなす。

【００１６】上記ルール情報に記述する不正アクセス判定基準は、例えば保護対象となるファイルの重要度と、当該重要度が割り当てられたファイルに対して許容できる異常アクセスの回数Ｎを規定したものであり、これにより、重要なファイルに対して異常アクセスが上記Ｎ回以上試みられた場合に悪意のあるアクセスであると判断する。あるいは、特定の同一ファイルに対する異常アクセスが上記Ｎ回以上試みられた場合に悪意のあるアクセスと判断してもよいし、更に他の基準として、同一のアクセス主体から異常なアクセスが上記Ｎ回以上試みられた場合に悪意のあるアクセスと判断してもよい。

【００１７】上記不正アクセス判定基準を満たした場合に実行すべき処理として、例えば、不正アクセスの要求元となる実行中のプログラムを強制的に終了させる旨を、上記ルール情報に記述する。これにより、重要なファイルに対して上記Ｎ回以上の異常なアクセスを試みたプログラムは、上記アクセス制御手段により強制的に終了される。

【００１８】また上記、不正アクセスの要求元となる実行中のプログラムからの以後のアクセスに対して、全てエラーを返す旨を、上記ルール情報に記述してもよい。これにより、重要なファイルに対して上記Ｎ回以上の異常なアクセスを試みたプログラムは、以後、発行するファイルアクセスは全て上記アクセス制御手段がエラーを返すことで却下される。

【００１９】また上記不正アクセスの要求元となる実行中のプログラムからの以後のアクセスを全てダミーファイルへのアクセスにリダイレクトし、当該ダミーファイルへのアクセスを監視・記録する旨を、上記ルール情報に記述してもよい。これにより、重要なファイルに対して上記Ｎ回以上の異常なアクセスを試みたプログラムからは、以後、発行するファイルアクセスが全て正常に処理されたようにみえるが、実際にはダミーファイルへのアクセスであるため、重要なファイルには被害が及ばない。

【００２０】また、上記アクセス制御ポリシーを切り替える旨を、上記ルール情報に記述してもよい。これにより、重要なファイルに対して上記Ｎ回以上の異常なアクセスが発生した場合、上記アクセス制御部は所定のアクセス制御ポリシーに切り替えて、以後のファイルアクセスをコントロールする。このとき、切り替え後のアクセス制御ポリシーを、切り替え以前のポリシーよりも制限の厳しいものとすることで、以後のファイルアクセスの正当性をより厳重にチェック可能となる。

【００２１】本発明のファイル保護システムによれば、上記ルール情報には、不正アクセス判定基準と当該基準を満たした場合に実行すべき処理との組み合わせ情報を、保護対象となるファイルの種類や重要度に応じて異なるものを指定することもできる。

【００２２】また、本発明を実現するのに必要な各プログラム（コード、モジュール、ユニットともいう）は、ネットワークに接続される他のサーバからコンピュータが読み取り可能な媒体、すなわちネットワーク上の伝送信号、またはＣＤ－ＲＯＭ、ＦＤなどの可搬型記憶媒体、を経由して、事前にまたは必要なときに導入してもよい。

【００２３】

【発明の実施の形態】以下、図を用いて本発明の実施の一形態を説明する。図１に、本発明の一実施形態が適用

された情報処理装置の構成を示す。情報処理装置１００は、ＣＰＵ１０、通信装置２０、入力装置２２、表示装置２５、外部記憶装置４０、主メモリ５０、バスなどの内部信号線５から構成され、アプリケーションプログラム８１などから上記外部記憶装置４０へのアクセスは、全てアクセス監視部６０によって監視されており、アクセス管理部８０による権限チェックを受け、許可された場合に限りＯＳ７０を介して処理される。上記アクセス管理部８０は、ポリシー情報６３、プロセス情報６１、ルール情報６４、ログ情報６５、異常アクセス集計情報６２を用いて、アクセス権チェック処理や不正アクセス防止策を実行する。上記外部記憶装置４０の記録媒体としては、ハードディスク、ＣＤ－ＲＯＭ、ＦＤ、ＭＯ、テープデバイスなどであってよい。また、これらの記憶媒体は、外部記憶装置４０に固定されたものでもよいし、可搬型であってもよい。また、外部記憶装置４０そのものが、独立したネットワークを構築したストレージ・エリア・ネットワーク（ＳＡＮ）であってもよい。

【００２４】ポリシー情報６３は、上記外部記憶装置４０内のデータに対する正常アクセスを定義したものである。プロセス情報６１は、現在実行中のプログラムに関する情報を格納したテーブルである。ルール情報６４は、異常なファイルアクセスのうち、悪意による不正アクセスを判別するための判定基準と、悪意による不正アクセスが発生したと判定した際に上記アクセス管理部８０がとるべき処理について規定したものである。ログ情報６５は、上記アプリケーションプログラム８１から上記外部記憶装置４０内のデータへのアクセスに関する証跡や、各種イベントに関する証跡を記録するためのものである。異常アクセス集計情報６２は、過去に発生したポリシー違反のアクセスに関する情報をリアルタイムに集計したものである。

【００２５】管理プログラム９０は、管理者により上記の各種情報６１～６５の参照や書き込み処理を行うために利用されるものである。管理プログラム９０は、上記アクセス管理部８０を経由して上記各種情報６１～６５にアクセスする。

【００２６】なお、上記ＯＳ７０は、ファイルシステムを標準で装備している基本ソフトウェアであり、本実施形態のファイル保護システムは、アクセス監視部６０と、アクセス管理部８０と、上記各種情報６１～６５と、管理プログラム９０から構成される。つまり、少なくともファイルシステムを備えた情報処理装置であれば、本実施形態のファイル保護システムの適用は可能である。

【００２７】また、上記アプリケーションプログラム８１は、例えばワープロソフトや、ブラウザ、インターネットサーバプログラムなど、多種多様なプログラムを意味している。上記ＯＳ７０と、アクセス監視部６０と、アクセス管理部８０と、アプリケーションプログラム８１と、管理プログラム９０は、それぞれ外部記憶装置４０またはネットワーク１３０を介して他の情報処理装置１０１から上記主メモリ５０にロードされ、実行するものである。ただし、ファイル保護システムが実行開始する前に、アプリケーションプログラムがファイルアクセスを実行することを避けるため、ＯＳが最初にロードされ、アプリケーションプログラム８１や管理プログラム９０よりも先に、アクセス監視部６０や、アクセス管理部８０がロードされる。このようなロードの順序は、ＯＳによってコントロールできる。

【００２８】以下では、上記ＯＳ７０がユーザーの識別・認証機能を備えており、上記アプリケーションプログラム８１は、上記機能により識別・認証されたユーザーの名義でファイルアクセスを実行するとの仮定のもとで、本発明の実施の一形態を示す。

【００２９】図２に、上記ポリシー情報６３の構成を示す。ポリシー情報６３は、ポリシーインデックス２００と、システムポリシー２１０と、ユーザーポリシー２２０と、エラーコード表２３０から構成される。ポリシーインデックス２００は、複数あるポリシーの識別情報と、現在有効なポリシーを索引するために必要な情報を格納したものである。

【００３０】システムポリシー２１０と、ユーザーポリシー２２０は、どちらも外部記憶装置内のファイルに対する正常なアクセスを定義したものであるが、システムポリシーとは、いかなる場合にも共通的なポリシーを記述したものであり、ユーザーポリシーとは、例えば「運用モード」「保守モード」「非常モード」のような情報処理装置１００の用途や状況に応じて、個別に記述されたポリシーである。したがって、ユーザーポリシーは、予めいくつかのモード毎にポリシーを登録しておき、適宜切り替えながら上記アクセス管理部８０がアクセス権をチェックすることが望ましい。

【００３１】エラーコード表２３０は、上記システムポリシーやユーザーポリシーのいずれかに違反したアクセスを発行したアプリケーションプログラム８１に対して、アクセス管理部８０からアクセス監視部６０を経由して返すべきエラーコードを記述したものである。

【００３２】図３に、上記ポリシーインデックスの一例を示す。ポリシーインデックス２００は、デフォルトのポリシーを識別するためのデフォルトフラグ３０１と、現在有効なポリシーを識別するための有効フラグ３０２と、ポリシーの識別番号３０３と、ポリシー名称３０４、各ポリシーの記載箇所を表すロケーション情報３０５からなる。上記デフォルトフラグ３０１は、有効フラグの初期値でもある。また、システムポリシーは常に有効でなければならないことから、デフォルトフラグ、有効フラグ共に「１」である。

【００３３】図４に、ポリシーの一例を示す。前述のように、ポリシーはシステムポリシー２１０とユーザーポ

リシー２２０とに大別できるが、記述形式は共通であり、保護対象の名称４０１と、その重要度４０２、アクセスタイプ４０３、プログラム名４０４、特徴値４０５、ユーザー名４０６、時間４０７から構成される。上記アクセスタイプ４０３には、Read（読み出し），Write（書き込み）の他に、Delete（消去），Rename（名称変更），Execution（実行），更に全てのアクセスタイプを含む「All」がある。保護対象の名称４０１は、ファイル単位だけでなく、ワイルドカードを用いた複数ファイル指定の他、フォルダ単位やドライブ単位でも指定できる。

【００３４】実際にポリシーを設定する際には、情報処理装置１００を利用する上で必要最小限のアクセスが何であるかを明らかにし、それらを正常アクセスとしてユーザーポリシーに登録することが重要である。また、上記重要度４０２の設定は、仮にそのファイルの内容が不当に改ざんされた場合または、漏洩した場合の被害の大きさを考慮して決めるものである。例えば、パスワードファイルや顧客リストが含まれるファイルには、インターネットから誰でも入手できるようなファイルよりも重要度を高く設定した方が良い。図４では、重要度が高いものほど大きい数値を設定している。

【００３５】プログラム名４０４には、上記保護対象へのアクセス手段として特別に許可されたプログラムを、当該プログラムファイルのパス名で指定する。特徴値４０５は、上記プログラムファイルがもつ特徴を数値化したものであり、ファイルサイズを指定しても良いし、プログラムファイルのハッシュ値を指定しても良い。これにより、プログラムの不正な改ざんを検知することができる。ユーザー名４０６は、アクセス要求元のプログラムがどのユーザーＩＤで実行されている場合にアクセスを許可するかを指定する部分である。上記ユーザー名４０６には、ユーザーＩＤの代わりにグループＩＤを指定しても良い。ユーザーＩＤとグループＩＤは、いずれもＯＳ７０が管理する情報である。

【００３６】時間４０７は、アクセスの可否とその時間帯を指定するところであり、例えば18:00から24:00の間に限りアクセスを許可したい場合は、「+18:00-24:00」と指定する。また、8:00から18:00の間はアクセスを禁止したい場合は、「-08:00-18:00」と指定する。図４の例を説明すると、ＣドライブのSec_Progディレクトリに含まれるファイル「C:¥Sec_Prog¥*」は全て保護対象であり、その重要度は「２」であることを表す。また、プログラム名が「C:¥prog¥Hsman.exe」であり、且つその特徴値が0x8A80であり、且つ上記プログラムがユーザーＩＤ「sec_admin」の権限で実行されているのであれば、18:00から24:00の時間帯に限り、上記C:¥Sec_Progディレクトリ下のファイルに対して「Read(読み出し)」と「Write(書き込み)」を許可することを意味している。

【００３７】上記ポリシーの構成要素のうち、重要度４０２と、アクセスタイプ４０３、プログラム名４０４、特徴値４０５、ユーザー名４０６、時間４０７については必ずしも全て指定する必要はない。アクセス管理部８０は、アクセス権チェックの際に指定されていない項目は無視する。以上説明したポリシーは、保護対象毎に正常なアクセスの条件を設定したものである。

【００３８】図１６に、他のポリシー設定例として、プログラム毎にアクセス可能な対象を設定したものを示す。プログラム名１６０１は、アクセス主体となるプログラムをパス名で表したものである。特徴値１６０２は、上記プログラムファイルがもつ特徴を数値化したものであり、図４で示した特徴値４０５と同じく、ファイルサイズを指定しても良いし、プログラムファイルのハッシュ値を指定しても良い。ユーザー名１６０３は、上記プログラム名１６０１で指定したプログラムがどのユーザーＩＤで実行されている場合にアクセスを許可するかを指定する部分である。

【００３９】上記ユーザー名１６０３には、図４で示したユーザー名４０６と同じく、ユーザーＩＤの代わりにグループＩＤを指定しても良い。アクセスタイプ１６０４では、図４で示したアクセスタイプ４０３と同じく、Read（読み出し）、Write（書き込み）の他に、Delete（消去）、Rename（名称変更）、Execution（実行）、更に全てのアクセスタイプを含む「All」から、上記プログラム名１６０１で指定したプログラムが実行可能なアクセスのタイプを選択できる。アクセス対象の名称１６０５は、上記プログラム名１６０１で指定したプログラムがアクセス可能な対象を表すものであり、ファイル単位や、ワイルドカードを用いた複数ファイル指定の他、フォルダ単位、ドライブ単位で指定できる。

【００４０】重要度１６０７は、図４で示した重要度４０２と同じく、仮にそのアクセス対象が不当に改ざんまたは、漏洩した場合の被害の大きさを考慮して設定するものであり、数値が大きいほど重要度は高い。時間１６０６には、図４で示した時間４０７と同じく、アクセスを許可された時間帯を設定する。図１６の例では、「C:¥prog¥editor.exe」というプログラムの特徴値が「0x3C77」をもち、且つ「users」というユーザーＩＤもしくはグループＩＤで実行されている場合、時間「8:00から18:00」の間に限り、「C:¥users¥*.txt」という名称のファイルに対して、Read（読み出し），Write（書き込み）、Delete（消去）のアクセスが可能となる。

【００４１】上記システムポリシー２１０とユーザーポリシー２２０は、上記図４で示した形式と図１６で示した形式のどちらを用いて設定してもよい。

【００４２】図４で示したポリシーの形式は、情報処理装置１００における保護対象が何であるかが明確となっていて、その用途を制限したい場合に有効である。これに対して図１６で示したポリシーの形式は、情報処理装

置１００にて利用されるプログラムが明確になっていて、それらプログラムによるアクセス可能な範囲を制限したい場合に有効である。

【００４３】ライブラリを動的にリンクしながら機能を拡張できるプログラムを例にとると、図１６で示したポリシーの形式を用いて、当該プログラムからリンク可能（Read可能）なライブラリファイルを制限することにより、プログラムの機能を制限することも容易になる。また、特定のライブラリファイルをリンク可能（Read可能）なプログラムを限定したい場合には、図４で示したポリシーの形式を用いればよい。

【００４４】以上説明したポリシー情報に記述されていない保護対象へのアクセスや、同じくポリシー情報に記述されていないプログラムの利用については、全面的に禁止しても良いし、あるいは全て許可しても良い。どちらにするかは、本発明のファイル保護システムを情報処理装置１００に導入する際に、情報処理装置１００の管理者が決定し、どちらを選択したのかについては、例えば環境設定情報として外部記憶装置４０内に保持しておき、アクセス管理部８０が参照できるようにしておけばよい。

【００４５】図５に、上記エラーコード表２３０の一例を示す。エラーコード表は、アクセスタイプ５０１とエラーコード５０２との対応表である。例えば上記アプリケーションプログラム８１から、あるファイルに対するReadアクセスがポリシー違反であった場合、上記アクセス管理部８０は、上記エラーコード表２３０を参照して、エラーコード「００１５」をアクセス監視部６０を経由して上記アプリケーションプログラム８１へ返す。上記エラーコード５０２には、上記ＯＳ７０が使用するものと同じものを登録しておく。

【００４６】図７に、上記プロセス情報６１の一例を示す。プロセス情報は、現在実行中のプログラムのプロセスＩＤ７０１と、プログラム名７０２と、ユーザー名７０３と、特徴値７０４と、起動日時７０５からなる。起動日時７０５は、同一の情報処理装置において過去にＯＳにより割り当てられ、利用されたプロセスＩＤが再度利用された場合にも、それらを区別できるように付与する。これらの情報は、プログラムが起動したときに上記アクセス管理部８０が取得して登録し、プログラムが終了したときに消去する。なお、本実施例では、実行中のプログラムをプロセス単位で扱っているが、スレッド単位であってもよい。

【００４７】図８に、上記ルール情報６４を設定するために、上記管理プログラム９０が提供するルール設定用グラフィカルユーザーインタフェース（ＧＵＩ）の一例を示す。当該ＧＵＩは、図１に示した表示装置２５に表示され、入力装置２２を用いて操作できる。情報処理装置１００の管理者は、ルール設定用ＧＵＩ８００を操作することで、悪意をもつ不正アクセスかどうかを判別するための判定基準８１０と、当該基準を満たした場合にとるべき防御処理８２０を設定できる。判定基準８１０には、例えば、以下に示す３つのタイプを用意し、この中から１つを選択する。

【００４８】１つ目のタイプは、重要度Ｌを割り当てられたファイル、ディレクトリ、またはドライブに対して、一定期間Ｔにポリシー違反がＮ回発生した場合に、悪意をもつ不正アクセスと判定するものである。この場合、管理者は図中の重要度指定ラジオボタン８１２を選択し、上記重要度Ｌを重要度入力ボックス８１３に指定し、一定時間Ｔを有効期間入力ボックス８１８に指定し、回数Ｎをポリシー違反回数入力ボックス８１７に指定する。図に示した例では、重要度３のファイル、ディレクトリ、またはドライブに対して、過去１時間（１ｈ）内に、ポリシー違反が３回以上発生した場合、アクセス元を問わず、アクセス管理部８０は、悪意のある不正アクセスと判定する。

【００４９】２つ目のタイプは、特定のファイル、ディレクトリ、またはドライブに対して、一定期間Ｔにポリシー違反がＮ回発生した場合に、悪意をもつ不正アクセスと判定するものである。この場合、管理者は図中のファイル指定ラジオボタン８１４を選択し、ファイル名、ディレクトリ名、またはドライブ名を名前入力ボックス８１５に指定し、一定時間Ｔを有効期間入力ボックス８１８に指定し、回数Ｎをポリシー違反回数入力ボックス８１７に指定する。図に示した例では、C:¥system¥passwdというファイルに対して、過去１時間（１ｈ）内に、ポリシー違反が３回以上発生した場合、アクセス元を問わず、アクセス管理部８０は、悪意のある不正アクセスと判定する。

【００５０】３つ目のタイプは、同一のプロセスから、一定期間Ｔにポリシー違反がＮ回発生した場合に、悪意をもつ不正アクセスと判定するものである。この場合、管理者は図中のプロセス指定ラジオボタン８１６を選択し、一定時間Ｔを有効期間入力ボックス８１８に指定し、回数Ｎをポリシー違反回数入力ボックス８１７に指定する。図に示した例では、同一のプロセスから、過去１時間（１ｈ）内に、ポリシー違反が３回以上発生した場合、アクセス管理部８０は、悪意のある不正アクセスと判定する。

【００５１】さらに、上記ルール情報６４に複数のルールを登録できるようにして、タイプの異なる判定基準を組み合わせた設定が可能となるように構成しても良い。

【００５２】以上の判定基準は、情報処理装置１００への侵入者が不正な目的を達成するために、例えばパスワードや、顧客リストが格納された重要なファイルに対して特に重点的にアクセスしてくる可能性が高いといった考えと、コンピュータウィルスに感染したプログラムからは多数のファイルに対して無差別的に不正なアクセスを連続して発行する傾向があるとの考えに基づく。この

ような悪意による不正ファイルアクセスは、ポリシー情報６３の設定だけでは防御できない可能性がある。例えばポリシー情報６３の設定により保護されていないファイルが存在するケースや、高度な知識をもつ攻撃者が、試行錯誤を繰り返しながら防御機構の抜け穴を見つけるケースである。

【００５３】しかし、過失または故意によるポリシー情報６３の未設定や防御機構の抜け穴に辿り着くまでには、多くのポリシー違反を繰り返す可能性が非常に高いと予想できる。したがって、上記判定基準を設定することにより、悪意をもつ不正アクセス主体が上記ポリシー情報６３の設定ミスや防御機構の抜け穴に辿り着く前に、アクセス管理部８０がその兆候を検出することが可能となる。

【００５４】次に、上記判定基準が満たされた場合（不正アクセスが発生した場合）に上記アクセス管理部８０がとるべき防御処理８２０の設定方法を示す。防御処理には、例えば以下の３種類あり、このうち２種類以上を組み合わせて指定することもできる。

【００５５】１つ目は、ポリシー切り替え処理である。管理者は図中のポリシー切り替え指定チェックボックス８２１を選択し、切り替え後の新たなポリシーをプルダウンメニュー８２２から選択して指定する。プルダウンメニュー８２２には、図３に示したポリシーインデックス２００内の、ポリシー名称３０４からシステムポリシーを除く全てのポリシー名称を、上記アクセス管理部８０が読み出して表示する。図に示した例では、上記判定基準を満たした場合、ポリシーを非常モードへ自動的に切り替える。実際に運用モードから非常モードへポリシーを切り替えるには、アクセス管理部８０が、上記ポリシーインデックス２００中の有効フラグ３０２を操作し、非常モードの有効フラグを「１」に、運用モードの有効フラグを「０」に書き換える。

【００５６】２つ目は、管理者への即時通知である。この場合、管理者は図中の管理者通知指定チェックボックス８２３を選択し、通知先を宛先アドレス入力ボックス８２４にて指定する。宛先アドレスは、管理者の電子メールアドレスや、リモートにある管理用ホストのアドレス、あるいは管理者が所持している電話番号でもよい。図に示した例では、上記判定基準が満たされた場合、その旨を管理者の電子メールアドレス(admin@hi-tech.com)に送信する。管理者への通知処理では、アクセス管理部８０が、上記通信装置２０とネットワーク１３０を経由して所定のアドレスに対してメッセージを送信する。当該メッセージには、悪意による不正アクセスが発生していると判断した理由（該当する判定基準）と、その対策内容（アクセス管理部８０がとるべき防御処理内容）を含める。

【００５７】３つ目は、上記判定基準のうち、プロセス指定ラジオボタン８１６を選択した場合において、当該判定基準を満たした不正アクセスを行ったプロセス（不正プロセスという）に対する処分である。この場合、管理者は図中の不正プロセスの処分指定チェックボックス８２５を選択し、更に、下記３つの処分方法の中から１つを選択する。

【００５８】ラジオボタン８２６は、上記不正プロセスによる以後のアクセスを全て禁止するときに指定する。この場合、アクセス管理部８０による具体的な処理内容は、上記不正プロセスからのアクセスに対して、アクセス権チェック処理をスキップして、上記ポリシー情報６３中のエラーコード表２３０から該当するエラーコードを読み出し、アクセス監視部６０を経由して上記不正プロセスに返す。

【００５９】ラジオボタン８２７は、上記不正プロセスを強制的に終了するときに指定する。この場合、アクセス管理部８０は、上記不正プロセスのプロセスＩＤを指定して上記ＯＳ７０に対するシステムコールを発行し、プロセスの強制終了を実行する。

【００６０】ラジオボタン８２８は、上記プロセスによる以後のアクセスを、すべてダミーファイルに対するアクセスに変換し、そのアクセスの監視と記録を行うときに指定する。この場合、アクセス管理部８０は、上記不正プロセスからのアクセスに対して、アクセス権チェック処理をスキップし、アクセス対象をダミーファイルへと変換し、アクセス監視部６０を経由して上記ＯＳ７０にフォワードする。また、ダミーファイルは上記外部記憶装置４０の中に予め用意しておき、そのファイルパス情報をアクセス管理部８０が保持しておく。

【００６１】最後に、ＯＫボタン８３０は上記設定内容をルール情報に登録する場合に押すべきボタンであり、キャンセルボタン８３１は上記設定内容を登録せずにルール設定用ＧＵＩ８００を終了する場合に押すべきボタンである。

【００６２】以上のように、設定した判定基準毎にその防御処理を設定できるので、例えば不正なアクセスを受けているファイルの種類や重要度に応じて、通知先のアドレスを変えることも可能となる。

【００６３】図９に、上記ルール設定用ＧＵＩ８００を用いて設定されたルール情報６４の一例を示す。図中には、構造が同じ３種類のルール（９１０，９２０，９３０）を含んでいる。各ルールは、ルール番号９０１と、判定基準コード９０２、重要度３、ファイル名９０４、ポリシー違反回数９０５、防御コード９０６、ポリシー識別番号９０７、通知先９０８、プロセスの処分９０９、有効期間９４０からなる。

【００６４】ルール番号９０１は、ルール情報６４に登録された複数のルールを識別するための番号である。判定基準コード９０２は、上記ルール設定用ＧＵＩ８００にて、判定基準として何れを選択したかを２進数３桁のビット列で表したものである。重要度指定ラジオボタン

８１２を選択した場合はビット列「１００」，ファイル指定ラジオボタン８１４を選択した場合はビット列「０１０」、プロセス指定ラジオボタン８１６を選択した場合はビット列「００１」となる。

【００６５】重要度９０３は、上記判定基準コードのビット列が「１００」の場合に登録されるものであり、その他の判定基準コードの場合は空（ＮＵＬＬ）とする。ファイル名９０４は、上記判定基準コードのビット列が「０１０」の場合に登録されるものであり、その他の判定基準コードの場合は空（ＮＵＬＬ）とする。ポリシー違反回数９０５には、上記ルール設定用ＧＵＩ８００のポリシー違反回数入力ボックス８１７に指定したものが格納される。防御コード９０６は、上記ルール設定用ＧＵＩ８００にて、防御処理８２０に何を選択したかを表すものである。

【００６６】防御コード９０６は、実行すべき防御処理を左から「ポリシー切り替え」、「管理者即時通知」、「不正プロセスの処分」の順に２進数３桁のビット列でコード化したものであり、選択されたものが「１」、選択されていないものが「０」である。ポリシー番号９０７は、上記ルール設定用ＧＵＩ８００のプルダウンメニュー８２２にて選択した新たなポリシーの識別番号であり、上記防御コード９０６のうち、「ポリシー切り替え」が選択されている場合に有効である。通知先９０８は、上記ルール設定用ＧＵＩ８００の宛先アドレス入力ボックス８２４にて指定した宛先アドレスであり、上記防御コード９０６のうち、「管理者即時通知」が選択されている場合に有効である。

【００６７】不正プロセスの処分９０９は、上記ルール設定用ＧＵＩ８００のラジオボタン８２６～８２８から選択した結果を２進数３桁のビット列でコード化したものであり、左から「アクセスを全て禁止」、「強制終了」、「アクセス監視と記録」の順に並んでおり、選択されたものが「１」、選択されていないものが「０」である。なお、プロセスの処分９０９に格納された情報は、上記防御コード９０６のうち、「不正プロセスの処分」が選択されている場合に有効である。また、有効期間９４０には、上記ルール設定用ＧＵＩの有効期間入力ボックス８１８に入力した期間Ｔが登録される。

【００６８】図６には、上記ログ情報６５の一例を示す。ログ情報には、上記アクセス管理部８０により、日時情報６１０、イベント情報６１１、イベント内容６１２といった情報が証跡として書き込まれる。上記イベント内容６１２には、当該アクセスが正常なアクセスだったのか、ポリシー違反だったのか、どのルール（番号）に該当するポリシー違反だったのか、あるいは不正プロセスによるダミーファイルへのアクセスであったのかを管理者が読んで分かるように記述する。

【００６９】また、上記ログ情報６５には、下記３種類がある。

【００７０】１つは、ファイルアクセスに関する情報であり、図中の６０１に示すように、日時、イベント、アクセス対象の情報、アクセス発行元の情報から構成される。これにより、いつ、何に、何が、どのようなアクセスを行ったのかが分かる。

【００７１】２つ目は、ポリシー切り替えに関する情報であり、図中の６０２に示すように、日時、イベント、切り替え後のポリシー名、切り替え前のポリシー名から構成される。これにより、いつ、どのポリシーから、どのポリシーへに、切り替えたのかが分かる。

【００７２】３つ目は、強制終了されたプロセスに関する情報であり、図中の６０３に示すように、日時、イベント、プロセス情報から構成される。これにより、いつ、どのプロセスが、強制終了されたのかが分かる。

【００７３】図１０には、集計情報６２の一例を示す。集計情報は、ポリシー違反のアクセスを集計したものであり、ルール番号１００１と、ポリシー違反回数１００２と、プロセス情報１００３、フラグ１００４、開始日時１００５からなる。ルール番号１００１は、上記ルール情報６４に登録された各ルールを識別するための情報である。ポリシー違反回数１００２は、ルールで指定した有効期間内に発生したポリシー違反回数を、ルール別に集計したものである。プロセス情報１００３は、プロセス指定の判定基準を設けたルールに利用されるものであり、ポリシー違反を発生したプログラムの名称やプロセスＩＤ、および起動日時を登録する。

【００７４】フラグ１００４は、上記判定基準を満たしているかどうかを、ルール別に示すものであり、判定基準を満たしている場合、つまり悪意による不正アクセスと思われるものに「１」を設定し、判定基準に達していないものには「０」を設定する。開始日時１００５は、ポリシー違反回数のカウントを開始した日時であり、アクセス管理部８０が、上記有効期間内に発生したポリシー違反の回数をカウントするために利用する。

【００７５】以上説明した各種情報は、例えば図１１に示すような情報一覧表示画面１１００を、上記管理プログラム９０が上記情報処理装置１００の表示装置２５に表示し、情報処理装置１００の管理者の操作を受け付けることによって、管理者は、現在の異常アクセスや不正アクセスの状況を把握したり、入力装置２２を操作しながらポリシーを手動で切り替えたりすることが可能となる。

【００７６】上記表示画面１１００は、ログ情報表示部１１０１と、当該ログ情報を並べ替えて表示するためのソートボタン１１０２と、集計情報表示部１１０３と、プロセス一覧表示部１１０４と、プロセス終了ボタン１１０５と、ルール情報表示部１１０６と、ルール追加ボタン１１０７と、ルール削除ボタン１１０８と、ポリシー表示部１１０９と、ポリシー切り替えボタン１１１０から構成される。

【００７７】上記ログ情報表示部１１０１は、上記ログ情報６５の内容を表示する部分であり、これにより、過去に発生したファイルアクセスや各種イベントの内容を確認できる。ソートボタン１１０２は、ログ情報を時系列だけでなく、アクセス対象（ファイル）やアクセス主体（プロセス）の名称で並べ替えたり、イベントの種類毎に並べ替えたりするために使われる。

【００７８】また、集計情報表示部１１０３からは、現在悪意による不正アクセスが発生しているかどうかを確認することができる。プロセス一覧表示部１１０４は、上記プロセス情報６１の内容を表示する部分であり、現在実行中のプロセスを確認できる。また、当該表示部１１０４からプロセスを選択して上記プロセス終了ボタン１１０５を押すことで、管理者の手動によるプロセス強制終了が可能となる。

【００７９】ルール情報表示部１１０６からは、現在登録されているルール情報６４の内容を確認でき、ルール追加ボタン１１０７を押すことで新規ルールの追加登録もできるし、ルール削除ボタン１１０８を押すことで、登録済みのルールを削除することもできる。図８に示したルール設定用ＧＵＩ８００は、上記ルール追加ボタン１１０７を押したときに、管理プログラム９０が表示するものである。

【００８０】ポリシー表示部１１０９からは、ポリシー情報６３に登録されているポリシーの一覧と、現在選択されているポリシーを確認することができる。また、ポリシー切り替えボタン１１１０を押すことで、ポリシーを手動で切り替えることもできる。このとき、上記アクセス管理部８０が、上記ポリシーインデックス２００中の有効フラグ３０２を書き換えることで、ポリシーが動的に切り替わる。

【００８１】以上のような管理者による操作は、セキュリティ上非常に重要であることから、上記管理プログラムの利用に先立って、例えば情報処理装置のＯＳが備える機能により、管理者の識別と認証処理を実行しておくことが望ましい。

【００８２】更に別の管理方法として、図１に示すように、上記管理プログラム９０とコマンドやデータを交換する機能と、上記管理プログラム９０と同様なユーザーインタフェースとを備えた管理マネージャ９１を、ネットワーク１３０で接続された他の情報処理装置１０１にて実行し、上記管理者は当該管理マネージャ９１が提供するユーザーインタフェースを操作しながら情報処理装置１００のログ情報確認や、ルール設定、ポリシーの手動切り替え等をリモートから行うといった実施形態も考えられる。

【００８３】図１２は、上記アクセス管理部８０による、プロセス監視処理内容について示したものである。アクセス管理部８０は、一般のアプリケーションプログラム８１や管理プログラム９０がロードされる前に、主メモリ５０上にロードされ、プロセス情報６１を格納するためのテーブルを作成し（ステップ１２０１）、プロセス監視処理を開始する（ステップ１２０２）。

【００８４】プロセスの起動を検知した場合、ステップ１２０３にてシステムポリシー２１０やユーザーポリシー２２０をチェックして、図４で示したプログラム名４０４または図１６で示したプログラム名１６０１に記載されていないプログラムのプロセス起動であれば、情報処理装置１００の管理者や利用者に対して警告メッセージを表示したり、当該プログラムを強制的に終了したりして、上記ステップ１２０６の処理をスキップしてプロセス監視処理（ステップ１２０２）へ戻る。

【００８５】上記システムポリシー２１０やユーザーポリシー２２０に登録されたプログラムのプロセス起動であれば、当該プロセスに関する情報を上記プロセス情報６１のテーブルに格納してから、プロセス監視処理（ステップ１２０２）へ戻る。

【００８６】プロセスの終了を検知した場合、ステップ１２０４にて、該当するプロセスの情報を上記プロセス情報６１のテーブルから削除する。次に、異常アクセス集計情報６２に上記プロセスに該当する情報があれば、ステップ１２０５にて削除し、プロセス監視処理（ステップ１２０２）へ戻る。

【００８７】本実施例では、情報処理装置１００にて利用するプログラムを制限するケースを想定してプロセス監視処理を示した。これにより、不正なプログラムの利用を積極的に防止できることから、高いセキュリティを実現できる。ただし、システムポリシー２１０やユーザーポリシー２２０には、予め情報処理装置１００にて利用可能なプログラムの名称が登録されているものとする。利用するプログラムを特に制限する必要がないのであれば、図１２で示したステップ１２０３の処理を常にスキップすればよい。利用するプログラムの制限の要否については、情報処理装置１００の管理者の判断に任せればよい。

【００８８】図１３は、上記アクセス監視部６０とアクセス管理部８０によるアクセス監視および不正アクセス対策の処理概要について示したものである。図中のステップ１３０２と、ステップ１３１２と、ステップ１３１３は、アクセス監視部６０の処理に含まれる。また、ステップ１３０３からステップ１３１１は、アクセス管理部８０の処理に含まれる。

【００８９】上記アプリケーションプログラム８１から上記外部記憶装置４０に格納されたファイルへのアクセスが発生すると、アクセス監視部６０が当該アクセスを検知し、ステップ１３０２にて、アクセス対象の名称と、アクセスのタイプと、当該アクセスの発行元となるプロセスＩＤを上記アクセス管理部８０へ通知する。アクセス管理部８０では、ステップ１３０３にて、上記通知されたプロセスＩＤを手掛かりに、当該プロセスのプ

ログラム名や起動日時をプロセス情報６１から取得する。

【００９０】次に、ステップ１３０４では、異常アクセス集計情報６２を参照することで、上記プロセスが上記ルール情報にて定義された判定基準を満たす不正プロセスでないことを確認する。ここで、不正プロセスでなければ、ステップ１３０５のポリシー照合処理に移るが、仮に不正プロセスだった場合には、ステップ１３０７へジャンプする。ステップ１３０５のポリシー照合処理の結果、ポリシーに適合した正当なアクセスであればステップ１３０６にて上記アクセス監視部６０に正常リターンを返す。アクセス監視部６０は正常リターンを受けると、上記ステップ１３１２にて、上記アプリケーションプログラム８１からのアクセス要求を、ＯＳ７０へフォワード（転送）する。

【００９１】上記ステップ１３０５のポリシー照合処理の結果、ポリシー違反と判定した場合、ステップ１３０７にて、アクセス内容をログ情報６５に記録する。次にステップ１３０８では、上記ポリシー違反となったアクセスが、ルール情報６４に登録されている何れかのルールに該当する場合、異常アクセス集計情報６２へ登録する。具体的には、図１０に示したポリシー違反回数１００２をインクリメントすると共に、開始日時１００５がルールで指定した有効期間内であるかどうかを確認する。

【００９２】上記有効期間より古い日時になっている場合には、期限内に発生したポリシー違反を、ログ情報６５を参照しながらカウントし直し、上記ポリシー違反回数１００２を修正する。同時に、現在の日時から上記有効期間を差し引いた日時を、上記開始日時１００５へ登録する。このようなアクセス管理部８０による不正アクセス集計処理は、ポリシー違反が発生したタイミングで実行しても良いし、ファイルアクセスとは関係なく定期的に実行するものであっても良い。

【００９３】ステップ１３０９では、上記ポリシー違反のアクセス発生によって、悪意による不正アクセスを判別するための判定基準（ルール情報６４に記載されている）に到達するかどうかを判定する。上記判定基準に到達していない場合には、ステップ１３１１にて、上記ポリシー情報６３中のエラーコード表２３０から該当するエラーコードを取得して、上記アクセス監視部６０にリターンする。アクセス監視部６０は、上記ポリシー違反のアクセスを発行したアプリケーションプログラム８１に対して、上記エラーコードを返し（ステップ１３１３）、アクセス監視処理に戻る。

【００９４】一方、上記判定基準に達した場合には、ステップ１３１０にてルール情報６４に記載されている所定の処理を実行してから、上記アクセス監視部６０によるアクセス監視処理に戻る。上記ステップ１３１０において実行した処理、例えばポリシー切り替えや、管理者への通知、不正プロセスの強制終了等については、上記ステップ１３０７と同様にアクセス管理部８０がログ情報６５に記録しておき、後で管理者によってトレースできるようにする。

【００９５】以上説明したファイル保護システムは、ポリシーに違反したアクセスの回数や、アクセス対象の重要度などから、悪意によると思われる不正アクセスをルール情報６４に基づいてに判定し、且つ対策を実施することができる。つまり、ポリシー情報６３に基づくファイルアクセス制御機能だけでなく、侵入やウィルス感染の兆候を不正アクセスのパターンから検出し、早期に対策を実施する機能まで提供することができる。

【００９６】図１４は、本実施形態のファイル保護システムを搭載した情報処理装置１００を用いて構成したインターネット・サイトおよびローカルエリアネットワーク（ＬＡＮ）の一例を示したものである。インターネットなどの外部ネットワークと内部ネットワークの間には、ファイアウォール１４０を設置することにより、外部ネットワークから利用なエリアであるＤＭＺ（De- Militarized Zone、非武装地帯、）１３０ａに設置された情報処理装置１００ａが提供するサービスは、インターネット１６０やＬＡＮ１３０ｂから利用できるが、インターネット１６０からＬＡＮ１３０ｂへのアクセスはできないよう制御できる。

【００９７】上記ＤＭＺ１３０ａに設置された情報処理装置１００ａは、例えばWWW(World Wide Web)サーバや、メールサーバ等のインターネットサーバである。また、ＬＡＮ１３０ｂに設置された情報処理装置１００ｂと情報処理装置１００ｃは、それぞれ例えば社内で利用する各種サーバや、業務用の端末装置として利用されるものである。

【００９８】ここで、上記ＤＭＺ１３０ａに設置された情報処理装置１００ａにて、例えばセキュリティホール（欠陥）をもつWWWサーバプログラムが動作している場合、当該セキュリティホールが悪用されて情報処理装置１００ａが侵入され、ホームページの改ざんやパスワードファイルの不正読み出しがなされる可能性がある。このような攻撃には、上記ファイアウォールだけでは対抗しきれないが、本実施形態のファイル保護システムを適用することにより、ユーザーＩＤだけでなく、アクセス手段となるプログラムや時間帯を制限できるため、侵入された場合にも被害を極小化できる。

【００９９】つまり、不正なファイルアクセスを未然に防ぐことができる。しかも、例えばパスワードファイルやホームページのファイルに対してポリシー違反のアクセスが一定時間内に連続して発生した場合に、当該アクセス発行元を強制的に終了するよう上記ルール情報６４を設定しておくことで、ファイル保護だけでなく、不正を行う可能性のあるプログラム（プロセス）を積極的に排除することも可能となり、安全なインターネットサー

ビスが提供できるようになる。

【０１００】このような不正アクセスは、インターネットだけでなく、社内ネットワーク（ＬＡＮ１３０ｂ）などのイントラネットにおいても発生しうる。本実施形態のファイル保護システムを、社内ＬＡＮの各サーバとなる情報処理装置１００ｂやクライアント（端末）となる情報処理装置１００ｃに適用することで、例えば顧客リストが格納された重要なファイルへのアクセスを監視して漏洩を未然に防いだり、不正なアクセスの発行元となるプロセスを排除したりできる。

【０１０１】また、ファイルを不正に消去したり、書き込みしたり、あるいは読み出して外部ネットワークへ送信するような悪質なコンピュータウィルスに対しても、そのファイルアクセスの状況から悪意による不正アクセスを検出可能であると共に、ウィルスに感染して不正なファイルアクセスを発行しているプロセスを検出し、強制的に終了させることも可能となる。また、本ファイル保護システムをクライアント（端末）に適用するのであれば、上記管理者への通知用メッセージを、クライアントである情報処理装置１００ｃの表示装置２５の画面上にも表示し、利用者に対して警告するものであってもよい。

【０１０２】更に、上記管理マネージャ９１を搭載した情報処理装置１０１を設置することで、上記ＤＭＺ１３０ａやＬＡＮ１３０ｂに設置された各情報処理装置に対して、リモートからルール設定やアクセス状況の監視、および手動によるポリシー切り替えも可能となる。

【０１０３】図１４には、更に他の適用例として、情報資産の保管場所となる外部記憶装置４０を、ストレージ・エリア・ネットワーク（ＳＡＮ）に置き換えた例も示している。図中のＳＡＮ１７０には、ハードディスクなどの記憶装置を複数台用いて高速、大容量で信頼性の高いディスク装置を実現したＲＡＩＤ(Redundant Arrays of Independent Disks)１７１や、テープライブラリ１７２が接続されている。上記情報処理装置１００ｂと各記憶装置（ＲＡＩＤ１７１，テープライブラリ１７２）との間は、スイッチ１７５により接続され、例えばファイバチャネル（ＦＣ）プロトコルなどを用いてデータ転送を行う。

【０１０４】この場合、情報処理装置１００ｂはＳＡＮのサーバとして、情報処理装置１００ｃから利用される。言い換えれば、ＳＡＮに接続されている記憶装置を利用するには、必ずＳＡＮサーバである情報処理装置１００ｂを経由する。現状、ＳＡＮのセキュリティ機能には、上記スイッチ１７５の機能を用いたゾーニングと呼ばれる記憶装置単位のアクセス制御技術と、ＬＵＮマスキングと呼ばれるＲＡＩＤ装置内のボリューム単位のアクセス制御技術が確立されている。ただしこれらの技術は、ＳＡＮのサーバ機器と、各記憶装置あるいはＲＡＩＤのボリュームとの間でのアクセス可否を管理するものであり、例えば利用者（ユーザーＩＤ）毎に、各記憶装置あるいはＲＡＩＤの各ボリュームへのアクセス可否を管理するものではない。

【０１０５】そこで、ＳＡＮのサーバに本実施形態のファイル保護システムを適用し、記憶装置やボリューム単位での正常なアクセスを、ＳＡＮサーバである情報処理装置１００ｂのポリシー情報６３に記述することで、ユーザーＩＤやプログラム名を組み合わせたきめ細かなアクセス管理が可能となる。これは、ＲＡＩＤ内のファイル単位のアクセスについても勿論同様である。

【０１０６】このようなポリシー情報を設定するためのポリシー編集画面の一例を図１５に示す。図中のポリシー編集画面１５００は、上記管理プログラム９０あるいは管理マネージャ９１が提供するＧＵＩであり、ＳＡＮのサーバとなる上記情報処理装置１００ｂの表示装置２５の画面上、もしくは管理マネージャ９１を搭載した情報処理装置１０１の画面上から管理者が操作するものである。当該編集画面は、保護対象選択部１５１０、保護対象直接指定部１５１５、プログラム選択部１５２０、その他の条件設定部１５３０からなる。

【０１０７】上記保護対象選択部１５１０では、記憶装置単位、ボリューム単位、ディレクトリ単位、ファイル単位で保護対象を表示選択できる。図中の例では、記憶装置「RAID-2」内のボリューム「Vol-1」内のディレクトリ「Doc¥Projects」下にあるファイル「idea.doc」を保護対象として選択している。これにより、ポリシー情報６３中の保護対象の名称４０１には、「RAID-2¥Vol-1¥Doc¥Projects¥idea.doc」が格納される。ただし、上記記憶装置のボリュームが、ある特定のドライブにマッピングしているのであれば、上記管理プログラム９０あるいは管理マネージャ９１が自動的に当該ドライブ名（例えばＤ：￥）に変換して「D:¥Doc¥Projects¥idea.doc」のように設定することも可能である。また、上記記憶装置単位の指定は、ＲＡＩＤやテープだけでなく、自他問わず情報処理装置が備えている外部記憶装置４０も指定可能なものである。

【０１０８】保護対象直接指定部１５１５は、保護対象をワイルドカードを用いて複数指定する場合に利用する。図中の例では、「RAID-2¥Vol-1¥Doc¥Projects¥*.doc」と指定されており、これはフォルダ「RAID-2¥Vol-1¥Doc¥Projects」の下にある拡張子が「.doc」のファイル全てを指している。保護対象選択部１５１０で選択したものと、保護対象直接指定部１５１５で指定したものが一致しない場合には、保護対象直接指定部１５１５で指定した方がポリシー情報６３中の保護対象の名称４０１に格納されるように構成すればよい。

【０１０９】プログラム選択部１５２０は、上記保護対象に対してアクセスを許可すべきプログラムファイルを選択指定する。図中の例では、「Prog¥office¥Sedit.exe」という名称のプログラムを選択しており、当該プロ

グラム名は、ポリシー情報６３のプログラム名４０４に格納される。その他の条件設定部１５３０では、保護対象の重要度と、許可すべきアクセスタイプと、ユーザー名/グループ名と、上記プログラムファイルの特徴値と、アクセス可能な時間帯とを指定する。

【０１１０】このうち特徴値については、プログラム選択部１５２０で選択されたプログラムファイルから、上記管理プログラムが自動的にその特徴値を導出して上記条件設定部１５３０に表示することで、管理者の手間を軽減できる。上記保護対象選択部１５１０、プログラム選択部１５２０、その他の条件設定部１５３０についてそれぞれ設定した後でＯＫボタン１５４０を押すと、設定項目がポリシー情報６３へ格納される。キャンセルボタン１５４１は、上記設定項目をクリアしたい場合に利用する。ポリシー編集画面１５００は、例えば図１１に示した情報一覧表示画面１１００にボタンを追加し、管理者が当該ボタンを押すことで呼び出し可能なものであっても良い。

【０１１１】以上説明したように、本実施形態によれば、情報処理装置にて発生するファイルアクセスのうち、ポリシー情報６３にて規定された正常アクセスに該当しないものを異常アクセスと見なして阻止できると共に、上記異常アクセスから更に悪意による不正アクセスを検出し、且つ防御処理を実行することにより、侵入やウィルス感染等の兆候を素早く検知して、その後予想される被害の発生を抑えることができるという効果がある。

【０１１２】また、柔軟なルール設定により、過失によるアクセスに対しては過剰な防御処理を不要とし、悪意による不正アクセスに対してのみ防御処理を実行できるという効果がある。特に、手当たり次第にファイルを破壊・削除するような悪質なプログラムを検出して強制終了するなどにより、早期発見から排除まで行えるという効果がある。

【０１１３】また、本実施形態において、ルール情報に登録しなければ、ポリシー情報に基づくファイルアクセス制御システムとして、セキュリティも重要だが処理スピードも重要視する分野に適用可能であり、ルール情報に登録してセキュリティを最重要視する分野に適用する場合とで、使い分けを行うことも可能である。

【０１１４】また、ユーザー識別・認証機能とファイルシステムとを備えたＯＳであれば、本実施形態のファイル保護システムを適用することで容易にセキュリティを強化できる。さらに、ファイアウォールや通信データ暗号機能等のセキュリティ技術と組み合わせることで、ネットワークシステム全体のセキュリティを向上させることができるという効果がある。

【０１１５】

【発明の効果】本発明によれば、情報処理装置が管理するファイルへの異常アクセスの内、悪意による不正アクセスを防ぐことが可能になる。

【０１１６】

【図面の簡単な説明】

【図１】本発明の実施の形態におけるファイル保護システムの一構成例を示す図。

【図２】ポリシー情報６３の一構成例を示す図。

【図３】各種ポリシーに関するインデックス情報を示す図。

【図４】ユーザーポリシー２２０の設定の一例を示す図。

【図５】エラーコード表２３０の一例を示す図。

【図６】ファイルアクセスや各種イベントを記録するためのログ情報６５の構造を示す図。

【図７】現在実行中のプロセスに関する情報を格納したプロセス情報６１の一例を示す図。

【図８】ルール情報６４を設定するための画面の一例を示す図。

【図９】設定されたルール情報６４の内部構造を示す図。

【図１０】異常アクセスの集計情報６２の一例を示す図。

【図１１】管理プログラム９０が表示装置に表示する管理用画面の一例を示す図。

【図１２】アクセス管理部８０によるプロセス監視とプロセス情報作成フローを示す図。

【図１３】アクセス監視部６０とアクセス管理部８０によるファイルアクセス制御と侵入検知処理のフローチャートを示す図。

【図１４】本実施形態のファイル保護システムを適用したネットワークシステムの一構成例を示す図。

【図１５】ポリシー情報６３を編集するための画面の一例を示す図。

【図１６】プログラム単位で設定したユーザーポリシー２２０の一例を示す図。

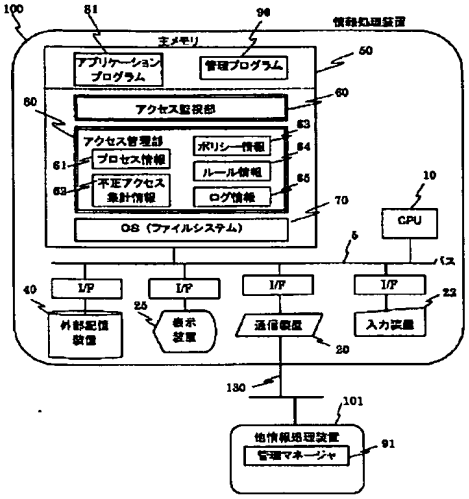
【符号の説明】

５…バス、１０…ＣＰＵ、２０…通信装置、２２…入力装置、２５…表示装置、４０…外部記憶装置、５０…主メモリ、６０…アクセス監視部、６１…プロセス情報、６２…異常アクセス集計情報、６３…ポリシー情報、６４…ルール情報、６５…ログ情報、７０…ＯＳ、８０…アクセス管理部、８１…アプリケーションプログラム、９０…管理プログラム、９１…管理マネージャ、１００…情報処理装置、１０１…他の情報処理装置、１３０…ネットワーク、１４０…ファイアウォール、１６０…インターネット、１７０…ＳＡＮ、１７１…ＲＡＩＤ、１７２…テープライブラリ、１７５…スイッチ、２００…ポリシーインデックス、２１０…システムポリシー、２２０…ユーザーポリシー、２３０…エラーコード表、８００…ルール情報設定用画面、１１００…情報一覧表示画面、１５０

０・・・ポリシー編集用画面

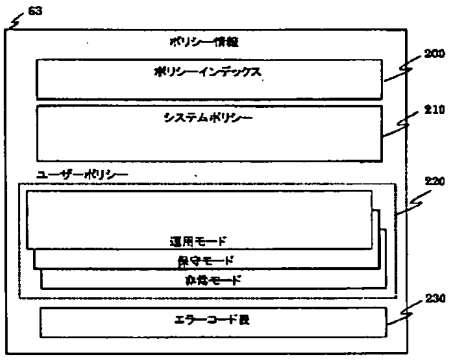
【図１】

図１



【図２】

図２



【図３】

図３

301 デフォルトフラグ	302 有効フラグ	303 識別番号	304 ポリシー名称	305 ロケーション情報
1	1	0000	システムポリシー	1－20
1	0	1010	運用モード	20 － 80
0	1	1020	保守モード	35 － 55
0	0	1030	非常モード	60 － 88

200 ポリシーインデックス

【図４】

220 保護対象の名称	401 重要度	402 アクセスタイプ A	X	N	D	W	R	403 プログラム名	404 特徴値	405 ユーザー名	406 時間	407
C:¥Sec_Prog¥*	2					*	*	c:¥prog¥Haman.exe	0x8A80	sec_admin	+18:00-24:00	
C:¥Prog¥*	1	*						c:¥prog¥Haman.exe	0x8A80	sec_admin	+00:00-24:00	
C:¥Prog¥sys*	1	*						c:¥prog¥Haman.exe	0x8A80	sec_admin	-08:00-18:00	
D:¥Doc¥*	3	*						c:¥prog¥Haman.exe	0x8A80	sec_admin	+00:00-24:00	

A: All
X: Execute
N: Rename
D: Delete
W: Write
R: Read

【図５】

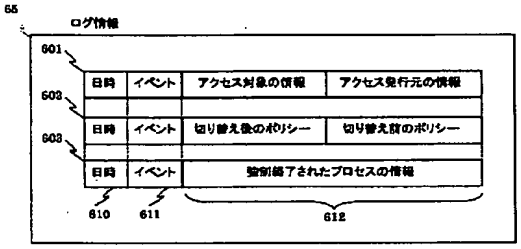
図５

230 エラーコード表

501 アクセスタイプ	502 エラーコード
Read	0015
Write	0018
Delete	0021
Rename	0024
Execute	0030
All	0050

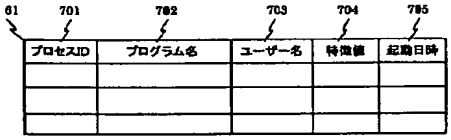
【図６】

図６



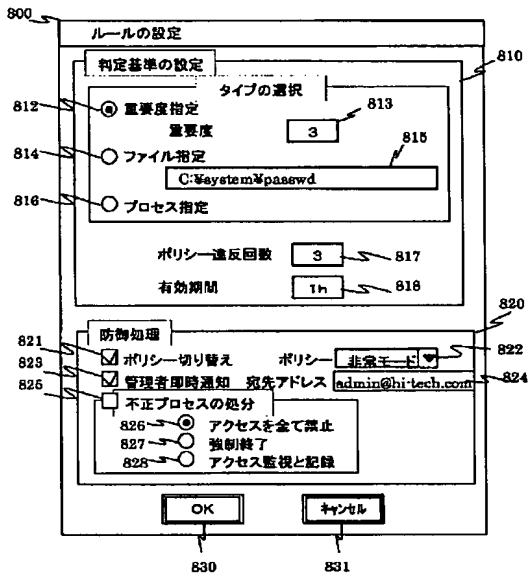
【図７】

図７



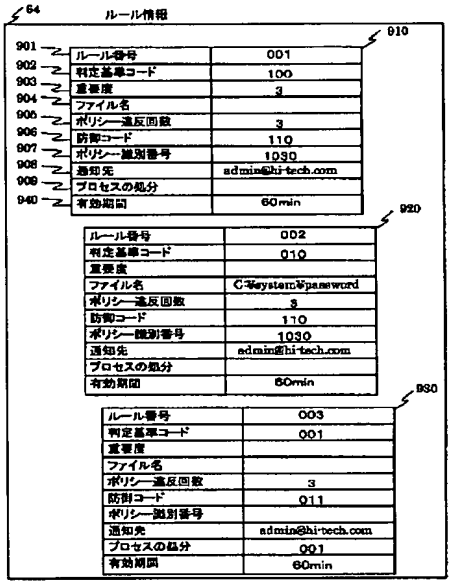
【図８】

図８



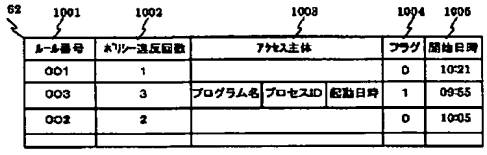
【図９】

図９



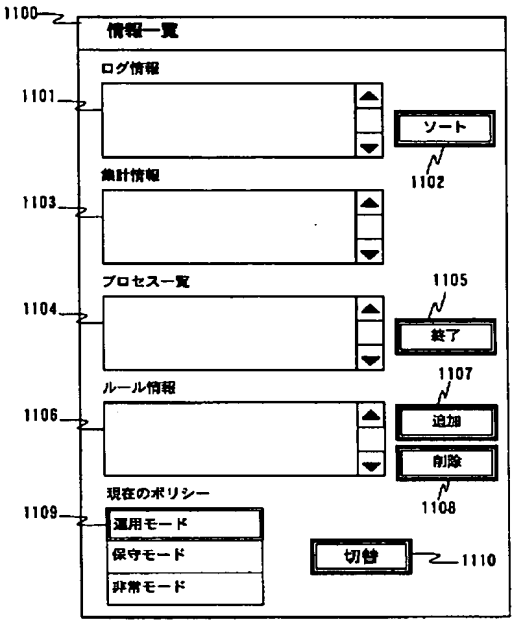
【図１０】

図１０



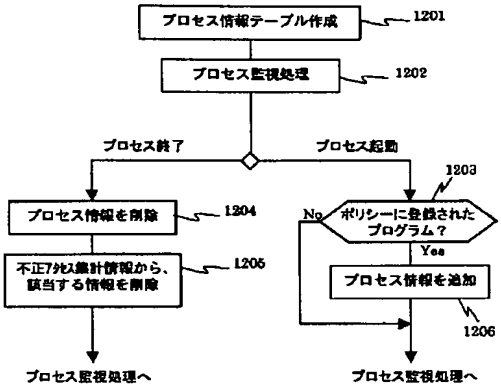
【図１１】

図１１



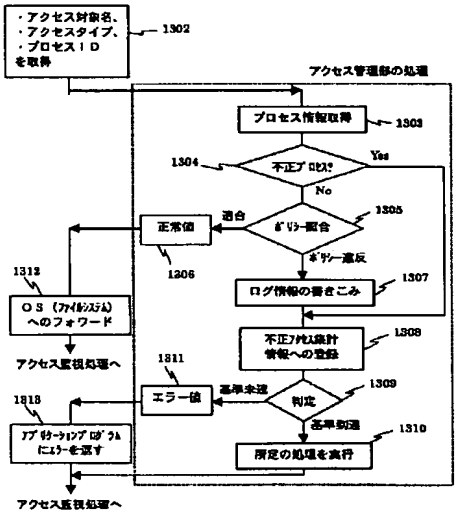
【図１２】

図１２



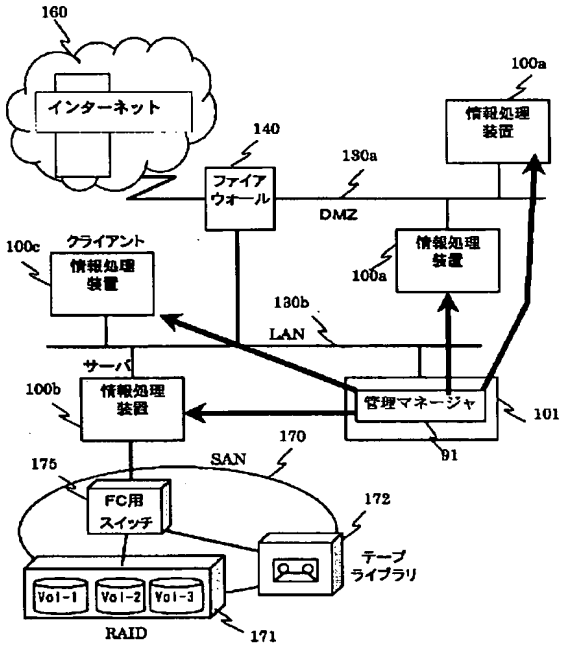
【図１３】

図１３



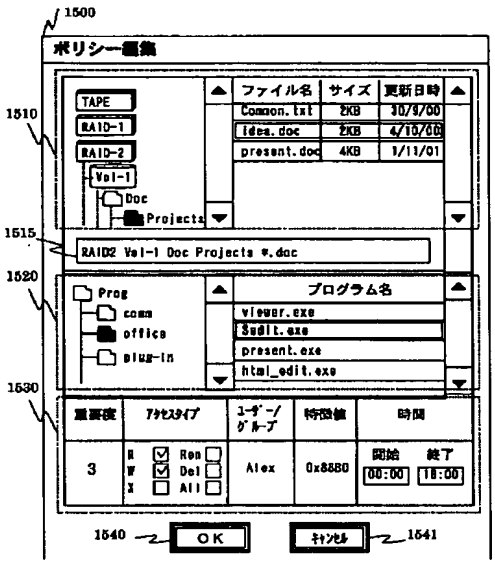
【図１４】

図１４



【図１５】

図１５



【図１６】

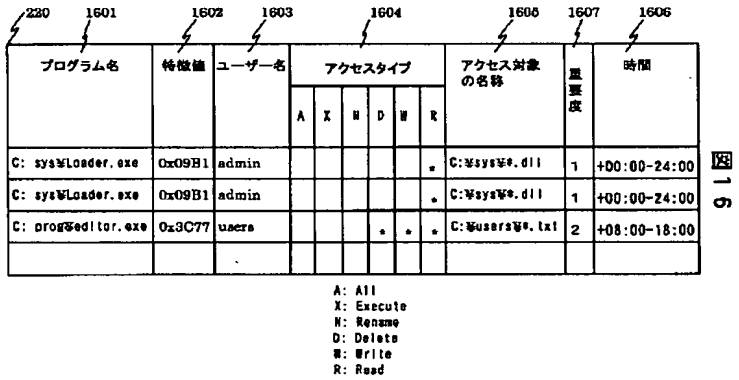


図16

フロントページの続き

Ｆターム(参考) 5B017 AA03 BA06 CA07 CA16
5B076 FB03
5B082 EA11